

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-245657
 (43)Date of publication of application : 19.09.1995

(51)Int.CI.

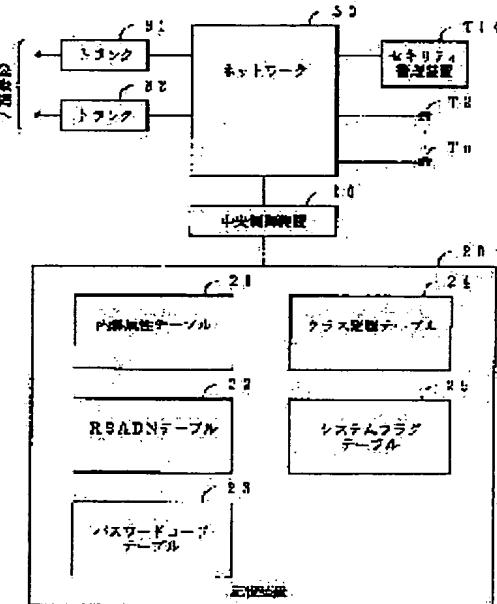
H04M 3/42
H04M 15/00(21)Application number : 06-035118
 (22)Date of filing : 07.03.1994(71)Applicant : FUJITSU LTD
 (72)Inventor : SUZUKI YUTAKA
 MOGI UMIHIKO

(54) REMOTE SYSTEM ACCESS CONNECTION RESTRICTION METHOD

(57)Abstract:

PURPOSE: To prevent surreptitious and illicit use of a password code by connecting an incoming call to a security management equipment of a private branch electronic exchange so as to confirm an extension class of the security management equipment thereby transferring the incoming call to an extension number (DN) for a remote system access(RSA).

CONSTITUTION: An incoming call from a remote location to a trunk 31 via a public network is connected to a security management equipment T10 of a private branch exchange and a qualification of a caller itself is confirmed through the matching between an ID code of the caller itself and a code using a date/time and a random number. Then an extension class of an equipment T10 is confirmed by using a network 30, a CPU 10, and a storage device 20 or the like having an extension attribute table 21, an RSADN table 22 and a pass word code table 23 or the like and a call from the equipment T10 to the RSADN is transferred, the access to the RSA is made and the service is started. Surreptitious and illicit use of a password code are prevented by using the security management equipment.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

THIS PAGE BLANK (USPTO)

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平7-245657

(43)公開日 平成7年(1995)9月19日

(51) Int.Cl. ⁶ H 04 M 3/42	識別記号 E C D 15/00	府内整理番号 F I Z	技術表示箇所
--	------------------------------	--------------------	--------

審査請求 未請求 請求項の数11 O.L (全 14 頁)

(21)出願番号 特願平6-35118	(71)出願人 富士通株式会社 神奈川県川崎市中原区上小田中1015番地
(22)出願日 平成6年(1994)3月7日	(72)発明者 鈴木 豊 神奈川県川崎市中原区上小田中1015番地 富士通株式会社内 (72)発明者 茂木 海彦 神奈川県川崎市中原区上小田中1015番地 富士通株式会社内 (74)代理人 弁理士 井桁 貞一

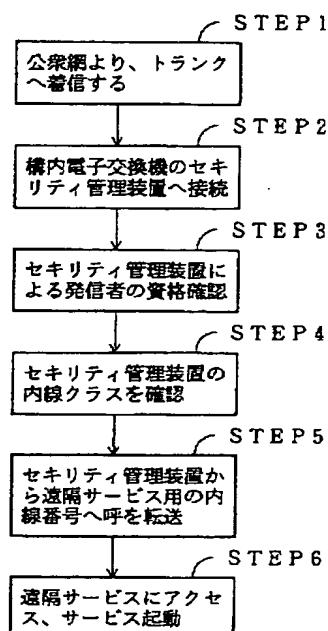
(54)【発明の名称】 遠隔システムアクセス接続規制方法

(57)【要約】

【目的】本発明は構内電子交換機の提供するサービスを公衆網から利用する際の接続規制方法に関し、パスワードコードの管理強化を可能とするセキュリティ管理装置を構内電子交換機に接続し、セキュリティチェックを強化することのできるRSA接続規制方法を実現することを目的とする。

【構成】STEP1で発信者からの呼が公衆網より構内電子交換機のトランクに着信し、STEP2でこの着信呼を構内電子交換機のセキュリティ管理装置T10に接続し、STEP3でセキュリティ管理装置T10により、発信者の資格を確認する。そして、STEP4ではセキュリティ管理装置T10の内線クラスを確認し、STEP5でセキュリティ管理装置T10がRSADNに転送可能な場合は、該着信呼をRSADNに転送し、STEP6は遠隔サービスにアクセスし、サービスを起動するように構成する。

本発明の原理を説明する図



【特許請求の範囲】

【請求項1】 構内電子交換機の提供するサービスを公衆網から利用する際の接続規制方法であつて、

発信者からの呼が公衆網より構内電子交換機のトランクに着信し(STEP1)、

次いで、該着信呼を、構内電子交換機のセキリティ管理装置(T10)に接続し(STEP2)、

前記セキリティ管理装置(T10)により、発信者の資格の確認を行い(STEP3)、

発信者の資格が遠隔システムアクセスを許可されている場合、前記セキリティ管理装置(T10)の内線クラスを確認し(STEP4)、

前記セキリティ管理装置(T10)の内線クラスが遠隔システムアクセスサービス用の内線番号(RSADN)に転送可能な場合には、該着信呼を前記セキリティ管理装置(T10)から遠隔システムアクセスサービス用の内線番号(RSADN)に転送し(STEP5)し、遠隔サービスにアクセスし、サービスを起動する(STEP6)、

ことを特徴とする遠隔システムアクセス接続規制方法

【請求項2】 前項記載の遠隔システムアクセス接続規制方法において、

記憶装置(20)に、構内電子交換機に収容される内線端末ごとのサービスクラスを定義する内線属性テーブル(21)と、

前記内線属性テーブル(21)で定義されるサービスクラスごとの接続規制内容を定義するクラス定義テーブル(24)を設け、

遠隔システムアクセスサービス用の内線番号(RSADN)に接続を行うとき、前記内線属性テーブル(21)に定義されたサービスクラスの接続可能サービスを前記クラス定義テーブル(24)より索引し、遠隔システムアクセスサービス用の内線番号(RSADN)に接続を行うことにより、遠隔システムアクセスサービスにアクセス可能な呼を内線からの転送呼に限定することを特徴とする請求項1記載の遠隔システムアクセス接続規制方法。

【請求項3】 1項記載の遠隔システムアクセス接続規制方法において、

前記遠隔システムアクセスサービス用の内線番号(RSADN)にアクセスするとき、自動的に外付けの前記セキリティ管理装置(T10)に接続するSTEP(20)、

を設けたことを特徴とする請求項1記載の遠隔システムアクセス接続規制方法。

【請求項4】 1項記載の遠隔システムアクセス接続規制方法において、

前記セキリティ管理装置(T10)から、遠隔システムアクセス用の内線番号(RSADN)に転送を行うとき、パスワードコードの入力が必要であるか否かを判定

するステップ(STEP30)、

を設けたことを特徴とする請求項1記載の遠隔システムアクセス接続規制方法。

【請求項5】 パスワードコードの設定と、受信したパスワードコードと設定しておいたパスワードコードとを比較可能な遠隔システムアクセスサービスを提供する構内電子交換機において、

遠隔システムアクセスへのアクセスを行うとき、パスワードコードごとに遠隔システムアクセス使用回数を計数し、そのアクセス回数が許容回数を越えるか否かを判定

するステップ(STEP50)を設け、
アクセス回数が許容回数を越える場合は以降の遠隔システムアクセスを禁止することを特徴とする遠隔システムアクセス接続規制方法。

【請求項6】 5項記載の遠隔システムアクセス接続規制方法において、

遠隔システムアクセスへのアクセスを行うとき、パスワードコードごとに遠隔システムアクセスで使用した料金を累積し、その使用累積料金が許容料金を越えるか否かを判定するステップ(STEP60)を設け、

アクセスの使用累積料金が許容料金を越える場合は以降の遠隔システムアクセスを禁止することを特徴とする請求項5記載の遠隔システムアクセス接続規制方法。

【請求項7】 5項記載の遠隔システムアクセス接続規制方法において、

遠隔システムアクセスへのアクセスを行うとき、遠隔システムアクセスの使用回数、および使用料金を計数する遠隔システムアクセスルーティング先を指定することを特徴とする請求項5記載の遠隔システムアクセス接続規制方法。

【請求項8】 パスワードコードの設定、比較と、録音装置(T20)へのルーティングが可能な遠隔システムアクセスサービスを提供する構内電子交換機において、遠隔システムアクセスへのアクセスを行うとき、RSA接続先スクリーニングテーブル(28)を照合し、前記RSA接続先スクリーニングテーブル(28)に指定される特定の遠隔システムアクセス先番号がダイヤルされた場合は前記録音装置(T20)に接続するステップ(STEP70)、を設けたことを特徴とする遠隔システムアクセス接続規制方法。

【請求項9】 8項記載の遠隔システムアクセス接続規制方法において、

遠隔システムアクセスへのアクセスを行うとき、RSA接続先スクリーニングテーブル(28)を照合し、前記録音装置(T20)への接続を行った際、システム管理用の多機能電話機(T30)に前記録音装置(T20)にルーティングされたことを通知するステップ(STEP80)、を設けたことを特徴とする請求項8記載の遠隔システムアクセス接続規制方法。

50 【請求項10】 8項記載の遠隔システムアクセス接続

規制方法において、

遠隔システムアクセスへのアクセスを行うとき、RSA接続先スクリーニングテーブル(28)を照合し、前記録音装置(T20)への接続を行った際、システム管理用の前記多機能電話機(T30)に前記録音装置(T20)にルーティングされたことを通知し、前記録音装置(T20)の録音内容から遠隔システムアクセスに使用されたパスワードコードを再生するステップ(STEP90)、を設けたことを特徴とする請求項8記載の遠隔システムアクセス接続規制方法。

【請求項11】 8項記載の遠隔システムアクセス接続規制方法において、

遠隔システムアクセスへのアクセスを行うとき、RSA接続先スクリーニングテーブル(28)を照合し、前記録音装置(T20)への接続を行い、該録音内容の再生により、不正使用と判定したときは、パスワードコードを無効とすることを特徴とする請求項8記載の遠隔システムアクセス接続規制方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は構内電子交換機の提供するサービスを公衆網から利用する際の接続規制方法に関する。

【0002】 電子交換機の技術の進展に伴い、構内電子交換機は単に構内電子交換機に収容された電話機相互間の通話のための交換接続を行うのみではなく、例えば、メールサービス、会議電話等の各種のサービスを提供するようになってきている。

【0003】 このような構内電子交換機が提供するサービスを遠隔地にいる発信者が公衆網を通してサービスを利用する遠隔システムアクセス(Remote System Access、以下RSAと称する)サービスが普及してきている。このサービスは、例えば、在宅勤務者や出張者等社外にいる発信者が自宅の電話や公衆電話から会社の構内電子交換機にアクセスし、この構内電子交換機の提供するサービスである会議通話、公衆網発信や音声メール等を利用するものである。

【0004】かかるRSAサービスにおいて、パスワードコードの盗用、悪用を防止することのできるRSA接続規制方法が要求されている。

【0005】

【従来の技術】 図13は従来例の構内電子交換システムを説明する図を示す。図中の10は中央制御装置であり、20は記憶装置であり、30はネットワークであり、31、32は公衆網に接続されるトランクであり、T1～Tnは端末である。

【0006】また、記憶装置20の中の22はRSAを利用するために内線番号群としてのRSADNテーブルであり、23はパスワードコードテーブルであり、パスワードコードごとに接続可能なRSAサービスが定義さ

れています。

【0007】図14は従来例のフローチャートである。以下フローチャートにしたがって、接続動作を説明する。STEP(以下sと略称する)11；遠隔地にいる発信者からの呼が、公衆網を経由して構内電子交換機のトランク31に着信し、構内電子交換機は受信したダイヤルを分析する。

【0008】s12；着信先がRSAサービスへの接続を行うために設けられた内線Aであるか否かを判定する。ここでは、端末T1が内線Aであるものとし、以下内線Aと称する。

【0009】s13；公衆網を経由する発信者と内線Aが接続される。

s14；内線Aがフッキングを行い、RSADNをダイヤルすると、内線Aにはダイヤルトーン(図中はDTと称する)が接続される。

【0010】s15；内線Aがオンフックする。

s16；内線Aのオンフックにより、トランク31にダイヤルトーンが送出され、発信者から送出されるパスワードコード(図中PWCと略称する)を受信する。

【0011】s17；パスワードコードがパスワードコードテーブル23に登録されているパスワードコードに一致するか否かを判定する。

s18；パスワードコードに一致した場合には、構内電子交換機のサービスの提供が可能であり、発信呼のクラスをパスワードコードのクラスに変更する。

【0012】s19；トランク31にダイヤルトーンを送出する。

s19a；発信者が送出するダイヤルを受信する。

s19b；指定されたサービスを起動する。

【0013】s12a；s12で着信先が内線Aでない場合、さらにRSADNへの着信であるか否かを判定し、RSADNへの着信の場合には、s15へ進む。

s12b；着信先が内線Aでなく、RSADNでもない場合は、通常の着信であるので通常の着信処理を行う。

【0014】s17a；s17でパスワードコードが一致しない場合は、RSAへの接続を行わずROT(Reorder Tone)接続を行う。

以上のような接続処理により、公衆網を経由した発信者が恰も構内電子交換機に収容されている端末T1～Tnと同等の状態におかれ、RSAサービスを受けることができる。

【0015】

【発明が解決しようとする課題】 上述の従来例において、RSAサービス接続の可否を判定するのは、パスワードコードの照合のみであり、RSAサービスを利用するためのパスワードコードが盗用あるいは悪用された場合、公衆網専用線-公衆網接続や公衆網-公衆網接続が許容されている環境においては、長距離通話や国際通話が不当に行われてしまい、構内電子交換機を所有して

いる会社に膨大な通話料金の支払いが請求されることがある。

【0016】本発明は、パスワードコードの管理強化を可能とするセキュリティ管理装置を構内電子交換機に接続し、セキュリティチェックを強化することのできるRSA接続規制方法を実現しようとする。

【0017】

【課題を解決するための手段】図1は本発明の原理を説明する図である。図はRSA接続規制方法を示し、STEP1で発信者からの呼が公衆網より構内電子交換機のトランクに着信し、STEP2で該着信呼を、構内電子交換機のセキュリティ管理装置T10に接続し、STEP3でセキュリティ管理装置T10により、発信者の資格の確認を行う。

【0018】さらに、STEP4で発信者の資格が遠隔システムアクセスを許可されている場合、セキュリティ管理装置T10の内線クラスを確認し、STEP5でセキュリティ管理装置T10の内線クラスが遠隔システムアクセスサービス用の内線番号RSADNに転送可能な場合には、該着信呼をセキュリティ管理装置T10から遠隔システムアクセスサービス用の内線番号RSADNに転送し、STEP6で遠隔サービスにアクセスし、サービスを起動する。

【0019】

【作用】公衆網を経由する発信者が構内電子交換機の提供する各種のサービスを利用するとき、公衆網から構内電子交換機のトランクに着信させた後、セキュリティ管理装置T10に接続する。この状態で発信者とセキュリティ管理装置T10が接続され、セキュリティ管理装置T10で、日時、乱数等により個人IDコードのチェックを厳重に行う。例えば、日時をキーとして乱数を発生する同じ乱数発生器を発信者、セキュリティ管理装置T10が持つており、発信者から送られてきた乱数がセキュリティ管理装置T10で発生した乱数と一致することを確認する。このようにして、公衆網を経由する発信者の資格はセキュリティ管理装置T10で厳重にチェックされた後、RSADNへ転送しサービスを起動する。

【0020】このように、RSADNへアクセスできる発信者はセキュリティ管理装置T10の厳重なる資格チェックで許可となった者のみであり、RSAへの不法なアクセスを防止することができる。

【0021】また、構内電子交換機に登録したパスワードコードごとに使用料金、使用回数を監視することにより、パスワードの盗用、悪用を防ぐことができる。さらに、特定のRSAアクセス番号がダイヤルされた場合、録音装置T20へのルーティングを可能にしておき、録音装置T20の録音内容から使用されたパスワードコードを確認することにより、パスワードの盗用、悪用を防ぐことができる。

【0022】

【実施例】図2は本発明の実施例の構内電子交換システム(1)を説明する図である。図中の10は交換処理を制御する中央制御装置であり、20は交換処理プログラム、各種テーブルを記憶する記憶装置、30は指定の端末相互間の接続を行うネットワークである。

【0023】また、31、32はトランクであり、T10は内線Aとして接続されるセキュリティ管理装置、T2～Tnは端末である。本発明において、記憶装置20には、内線のクラス属性を定義する内線属性テーブル21、RSAサービスを利用するための内線番号群としてのRSADNテーブル22、発信者の資格を確認するためのパスワードコードテーブル23、サービスクラスごとに利用可能なサービスを定義するクラス定義テーブル24、各種システムフラグを定義するシステムフラグテーブル25が設けられている。

【0024】

図3は本発明の実施例のテーブル構成(1)を説明する図である。(A)は内線属性テーブル21の構成を示し、各内線ごとにサービスクラス(Class Of Service、以下COSと略称する)、接続規制クラス(Restriction Mode、以下RSMと略称する)、ファシリティ規制クラス(Facility Restriction Level、以下FRLと略称する)の値が定義され、(B)はRSADNテーブル22の構成を示し、各RSADNごとにサービスクラスCOS、接続規制クラスRSM、ファシリティ規制クラスFRLおよびセキュリティグループ番号(Security Group、以下SGRPと略称する)の値が定義されている。このセキュリティグループ番号(SGRP)は番号ごとにセキュリティ用のパスワードコード群を定義するための管理番号である。

【0025】また、(C)はパスワードコードテーブル23の構成を示し、パスワードコード(Pass Word Code、以下PWCと略称する)、およびパスワードコードPWCとしてのサービスクラスCOS、接続規制クラスRSM、ファシリティ規制クラスFRLの値が定義され、(D)はクラス定義テーブル24の構成を示し、サービスクラスCOSごとにどのサービスが可能であるかを定義し、(E)はシステムフラグテーブル25の構成を示し、RSAサービスへの直接アクセス許容フラグ251、セキュリティ管理装置T10への自動迂回フラグ252およびパスワードコード省略フラグ253が格納されている。

【0026】

図4は本発明の実施例のフローチャート(1)を示す。図は請求項1、2に対応する実施例のフローチャートであり、以下フローチャートにより本発明の動作を説明する。

【0027】STEP(以下Sと略称する)11；遠隔地にいる発信者からの呼が公衆網を経由して構内電子交換機のトランク31に着信し、構内電子交換機は受信したダイヤルを分析する。

【0028】S12；着信先がRSAサービスを行うた

めに設けられた内線Aであるか否かを判定する。ここでは、内線Aに外付けのセキュリティ管理装置T10が接続されているものとする。

【0029】S13；公衆網を経由する発信者とセキュリティ管理装置（図中はセキュリティ装置と略称する）T10が接続され、自動応答し二者通話状態となる。このとき、セキュリティ管理装置T10から発信者へIDコード等を入力することを指示するメッセージを送出し、セキュリティ管理装置T10は発信者からのIDコード等を受信し、一連の資格チェックを行う。

【0030】S14；セキュリティ管理装置T10による資格チェックの結果、正当な利用者と判断した場合は、セキュリティ管理装置T10はフッキングを行い、RSAサービス専用の電話番号RSADNを送出する。

【0031】S15；中央制御装置10は転送先がRSADNであることから、内線AのサービスクラスCOSを内線属性テーブル21から読み出し（ここではCOS=0）、クラス定義テーブル24のRSA転送が許容されているか否かを判定し、許容されていない場合にはS15aへ進む。

【0032】S16；RSA転送が許容されている場合には、発信呼のクラス属性を一時的に内線Aのクラス属性に置き換える。

S17；RSADNへ仮想的に接続され、ダイヤルトーン（図中DTと示す）を接続し、内線Aをオンフックする。

【0033】S18；内線Aがオンフックすることにより、トランク31とRSADNとが仮想的に接続され発信者はダイヤルトーンを聴取する。

S19；ダイヤルトーンを聴取し、発信者は希望するサービスにアクセスするコード、あるいは、公衆網に発信する場合は、公衆網に発信するアクセスコードおよび相手先番号をダイヤルする。

【0034】S19a；中央制御装置10は指定のサービスの起動あるいは公衆網に接続するためにトランク32を起動し接続動作を行う。

S12a；S12で着信先が内線Aでない場合は通常の着信があるので通常の着信処理を行う。

【0035】S15a；S15でRSAへの転送を許可されていない場合は、RSAへの接続を行わずROT接続を行う。

このような手順により、公衆網を経由しRSAサービスへアクセスする発信者の資格をセキュリティ管理装置T10で確実にチェックすることにより、不法なアクセスを防止することができる。さらに、RSADNへの転送を行うとき、該内線のサービスクラスをクラス定義テーブル24を参照し、転送が許容されている内線であるか否かを判定することにより、RSADNへの転送可能とする内線を限定することができる。

【0036】図5は本発明の実施例のフローチャート

（2）を示す。図は請求項3、4に対応する実施例のフローチャートであり、RSADNに直接着信してきた場合、自動的に外付けのセキュリティ管理装置T10に接続するためのステップ20としてのS21～S23、およびRSADNに転送するときパスワードコードの入力が必要か否かを判定するステップ30としてのS31～S35を設けたものである。以下フローチャートにより動作を説明する。

【0037】S11；発信者からの呼が構内電子交換機のトランク31に着信し、受信したダイヤルを分析する。

S12；着信先がRSAサービスを行うために設けられた内線Aであるか否かを判定する。ここでは、内線Aへの着信でない場合はS21へ進む。

【0038】S21；内線Aへの着信でない場合、次いで、RSADNへの着信か否かを判定し、RSADNへの着信でない場合、S13aへ進む。

S22；さらに、システムフラグテーブル25を参照して、RSAへの直接アクセス許容フラグ251が立っているか否かを判定し、立っていない場合はS15aへ進む。

【0039】S23；システムフラグテーブル25を参照して、セキュリティ管理装置T10への自動迂回フラグ252が立っているか否かを判定し、立っていない場合はS13へ進む。

【0040】S13～S17；着信先が内線Aの場合、セキュリティ管理装置T10が接続され、セキュリティ管理装置T10は発信者からのIDコード等を受信し、一連の資格チェックを行った上でRSAサービス専用の電話番号RSADNを出し、内線AのサービスクラスCOSがRSA転送が許容されているか否かを判定し、許容されている場合には、発信呼のクラス属性を一時的に内線Aのクラス属性に置き換える。

【0041】S31；システムフラグテーブル25を参照して、パスワードコード省略フラグ253が立っているか否かを判定し、省略可の場合にはS18へ進む。

S32；パスワードコードの入力を省略できない場合は、トランク31にダイヤルトーンを接続し、パスワードコードの入力を指示する。

【0042】S33；発信者からのパスワードコードを受信する。

S34；中央制御装置10は受信したパスワードコードがRSADNテーブル22に格納されているパスワードコード群の中のものと一致するか否かを判定し一致しない場合はS15aに進む。

【0043】S35；パスワードコードが一致した場合は、発信呼のクラスをパスワードコードのクラスに変更し、S18へ進む。

S18～S19a；発信者は希望するサービスにアクセスするコードを入力することにより、サービスを起動す

る。

【0044】このような手順により、内線転送呼以外の呼がRSADNにアクセスしようとするとき、自動的に外付けのセキュリティ管理装置T10が接続されている内線Aにルーティングするとともに、RSADNにアクセス可能な呼を内線からの転送呼に限定することができる。

【0045】また、本実施例においては、外付けのセキュリティ管理装置T10において、厳重なる資格チェックが可能であるので、パスワードコードの入力をスキップし、指定のRSAサービスへアクセスすることができる。

【0046】図6は本発明の実施例の構内電子交換システム(2)を説明する図である。図は図2で説明した構内電子交換システム(1)の中央制御装置10に、各種テーブルのデータを設定するデータ設定部11、各種接続動作の回数をカウントするカウンタ12、データ接続部11で設定した値とカウンタ12によるカウント値を比較するデータ比較部13、詳細課金情報制御部10Aとのインターワークを行う課金情報インターワーク部(図中課金情報INTと称する)14を設け、記憶装置20には各種データを設定するデータテーブル26を設けたものである。

【0047】図7は本発明の実施例のデータテーブルを説明する図である。データ設定部11によりデータテーブル26の中にパスワードコードごとに次のデータを設定する。

【0048】ルーティング先番号ごとの局線トランク発信許容回数。

ルーティング先番号ごとの局線トランク発信使用回数。

ルーティング先番号ごとの専用線トランク発信許容回数。

【0049】ルーティング先番号ごとの専用線トランク発信使用回数。

、を含むRSAアクセスから利用可能な構内電子交換機のサービスへアクセス可能な許容回数。

【0050】、を含むRSAアクセスから利用可能な構内電子交換機のサービスへアクセスした回数。

におけるサービスアクセスの累積使用料金の上限。

【0051】におけるサービスアクセスの実際に使用した料金の累計。図8は本発明の実施例のフローチャート(3)を示す。図は請求項5、6に対応する実施例のフローチャートであり、STEP50とSTEP60としてのST60'～ST64を設けたものであり、以下フローチャートにより本発明の動作を説明する。

【0052】S50; RSAへアクセスを行うとき、データテーブル26の中のパスワードコードごとのRSAサービス(図中はRSASと示す)トータルアクセス使

用回数がトータルアクセス許容回数未満か否かを判定し、許容回数を越えた場合はS64に進む。

【0053】S60';さらに、データテーブル26の中のパスワードコードごとのサービスアクセスに使用した料金の累計がアクセスの累積使用料金の上限未満か否かを判定し、使用料金の上限を越えた場合はS64に進む。

10 【0054】S60a;アクセスするRSAサービスは局線発信/専用線発信の何れかであるか否かを判定し、否の場合にはS61へ進む。

S60b; RSAルーティング先番号はデータテーブル26の中に登録されているか否かを判定し、否の場合にはS64に進む。

【0055】S60c; RSAルーティング先番号のデータテーブル26の中の発信使用回数は許容回数以下か否かを判定し、否の場合にはS64に進む。

S61;許容の場合にはデータテーブル26の使用したルーティング先番号の使用回数を「+1」カウントする。

20 【0056】S62; RSAサービスへのトータルアクセス回数を「+1」カウントする。

S63;サービス終了後、RSAサービスの使用料金を累積する。

S64;該サービスをロックとし、アクセスしてきた発信者に対して、トーン、アナウンス等によりロックとしたことを通知する。

【0057】S60cで、ルーティング先番号ごとに使用回数を許容回数と比較し、使用可否を決めているが、ルーティング先番号ごとに使用料金の累計を累積使用料金の上限と比較し、使用可否を決めることも可能である。

【0058】また、図7のデータテーブルのようにテーブルを構成することにより、遠隔システムアクセスのルーティング先を任意に設定することができる。例えば、「03」と指定すれば、「03」で始まるすべての番号をルーティング先として指定することが可能となる。

(請求項7対応)

図9は本発明の実施例の構内電子交換システム(3)を説明する図である。図は図2で説明したRSADNテーブル22、パスワードコードテーブル23を備える記憶装置20に、表示機能付き多機能電話機T30のボタン情報を管理する多機能電話ボタンテーブル27、RSAアクセス呼を録音装置T20にルーティングする宛先呼を格納したRSA接続先スクリーニングテーブル28、特定の発信者からの呼以外を自動的に録音装置T20にルーティングさせるための発信者番号を定義した発信者スクリーニングテーブル28A、メッセージ番号、使用フラグ等を書き込むRSA録音メッセージテーブル29を設け、ネットワーク30には録音装置T20、システム管理者用の表示機能付き多機能電話機T30を接続し

たものである。

【0059】図10は本発明の実施例のテーブル構成(2)を説明する図である。RSA-DNテーブル22、パスワードコードテーブル23は図3と説明したと同じ内容であるので説明は省略する。

【0060】(A)は多機能電話機ボタンテーブル27の構成を示し、各多機能電話機の内線ごとに実装されているボタンの機能が定義されている。例えば、ここでは、多機能電話機T30は構内電子交換機の内線Bに接続されており、そのボタン00は主回線に、ボタン02はRSA管理に割り当てられている。(B)はRSA接続先スクリーニングテーブル28の構成を示し、RSAアクセス呼を録音装置T20に接続するべき宛先コードが格納されており、このテーブルに定義された宛先番号がトランク31から受信された場合には録音装置T20に自動的に接続する。

【0061】また、(C)は発信者スクリーニングテーブル28Aの構成を示し、自動ルーティングを行わない発信者番号群が格納されており、(D)はRSA録音メッセージテーブル29の構成を示し、メッセージ番号、使用中フラグ(0;未使用、1;使用中)、パスワードコード(PWC)、ダイヤルされた番号、呼が発生した日時および再生フラグ(0;未再生、1;再生済)が書き込まれる。

【0062】図11は本発明の実施例のフローチャート(4)を示す。図は請求項8、9に対応する実施例のフローチャートであり、RSA呼が着信したときの処理フローチャートであり、STEP70としてのST71～ST78とSTEP80を設けたものである。以下フローチャートにより本発明の動作を説明する。

【0063】S11～S19；トランク31へ着信し、ダイヤル受信した数字がRSA-DNテーブル22内に格納されているコードのどれかと一致した場合、RSA-DNへ仮想的に接続されDTが送出される。発信者はパスワードコードを入力し、パスワードコードが一致した場合、さらにサービスにアクセスするコードまたは公衆網に発信するアクセスコードと相手先番号をダイヤルすることでトランク32を起動し接続が完了する動作は図5のフローチャートで説明したのと同じ動作である。

【0064】S71；受信したアクセスコードがトランクにアクセスするコードか否かを判定し、否の場合にはS71aへ進む。

S72；RSA接続先スクリーニングテーブル28を検索する。

【0065】S73；受信した宛先コードがRSA接続先スクリーニングテーブル28の内容と一致しない場合はS19aに進む。

S74；受信したコードが本テーブル内に格納されている宛先コードと一致する場合は、この呼を録音装置T20に接続し、使用中フラグが「0」であるメッセージ番

号を探し、該メッセージ番号に使用中フラグ「1」を立てる。

【0066】S75；発信者に対し予め決められた合言葉の入力を促すためのトーンあるいはアンウンスを送出する。

S76；トランク31をメッセージ番号に対応する録音ポートに一定時間接続する。

【0067】S77；RSA録音メッセージテーブル(図中RSA録音テーブルと略称する)29に受信したパスワードコード、宛先番号、現在日時情報を格納する。

S78；一定時間経過後に録音ポートを解放し、その旨を示すトーンあるいはアンウンスを送出する。

【0068】S80；多機能電話機T30のRSA管理ボタンに対応するボタンのランプを点滅させることで、システム管理者に録音装置T20経由で発信したRSA呼が発生し、メッセージが残されたことを通知する。

【0069】図12は本発明の実施例のフローチャート(5)を示す。図は請求項10、11に対応する実施例のフローチャートであり、録音装置T20の録音内容を再生する処理フローチャートであり、STEP90としてのST91～ST99を設けたものである。以下フローチャートにより本発明の動作を説明する。

【0070】S80；多機能電話機T30のRSA管理ボタンのランプ点滅(図11のS80に同じ)。

S91；多機能電話機T30のRSA管理ボタンを押下げる。

【0071】S92；多機能電話機T30と録音装置T20が接続される。

S93；多機能電話機T30に使用フラグ「1」、再生フラグ「0」の未再生のメッセージ番号に対する録音メッセージの内容を送出し、多機能電話機T30の表示部に該メッセージ番号に対応するパスワード呼、宛先番号および日時を表示する。

【0072】S94；一定時間後に録音ポートを解放し、その旨を示すトーンあるいはアンウンスを送出する。

S95；多機能電話機T30のダイヤルにより次の選択が可能となる。

【0073】S95a；メッセージ内容が正当か否かの判定を保留し、後で確認する場合。

*を入力する。本メッセージは未再生のまま残される。メッセージ番号対応の使用中フラグ「1」、再生フラグ「0」と設定する。

【0074】S95b；メッセージ内容が正当な場合。#を入力する。本メッセージはクリアされ、メッセージ番号対応の使用中フラグ「0」、再生フラグ「0」と設定する。

【0075】S95c；メッセージ内容が不当な場合。99を入力する。本メッセージはクリアされ、メッセー

ジ番号対応の使用中フラグ「0」、再生フラグ「0」と設定する。

【0076】S96；このとき、該当のパスワードコードは盗用または悪用されたものと判定し、パスワードコードテーブル23より削除する。

95d；上記コードを入力せずに多機能電話機T30を切断した場合は、95aが設定されたものとして処理する。

【0077】S97；未再生メッセージが有るか否かを判定し、存在している場合は92に戻る。

10

S98；未再生メッセージがない場合には終了トーンを送出する。

【0078】S99；切断を行う。

上述の処理によりパスワードコードの悪用、盗用を防止することができる。

【0079】

【発明の効果】本発明によれば、構内電子交換機が提供する各種サービスを公衆網から利用するRSAサービスにおいて、セキュリティ装置との連携を行い、セキュリティ装置を経由した呼のみにRSA接続を許容することにより、セキュリティチェックを強化することができる。

【0080】また、パスワードコードごとに利用上限を設定し、上限を超えない範囲でRSAサービスの利用を許容することで、膨大な料金の不法アクセスを制限することができる。

【0081】さらに、特定宛先に発信する呼や不特定の発信元からの呼に対しては音声による合言葉を録音し、確認することにより正当性を確実にチェックすることが可能となる。

【図面の簡単な説明】

【図1】本発明の原理を説明する図

【図2】本発明の実施例の構内電子交換システム

(1)を説明する図

【図3】本発明の実施例のテーブル構成(1)を説明する図

【図4】本発明の実施例のフローチャート(1)

【図5】本発明の実施例のフローチャート(2)

【図6】本発明の実施例の構内電子交換システム

(2)を説明する図

【図7】本発明の実施例のデータテーブルを説明する図

【図8】本発明の実施例のフローチャート(3)

【図9】本発明の実施例の構内電子交換システム(3)を説明する図

【図10】本発明の実施例のテーブル構成(2)を説明する図

【図11】本発明の実施例のフローチャート(4)

【図12】本発明の実施例のフローチャート(5)

【図13】従来例の構内電子交換システムを説明する図

【図14】従来例のフローチャート

【符号の説明】

10 中央制御装置

11 データ設定部

12 カウンタ

13 データ比較部

14 課金情報インターワーク部

20 10A 詳細課金情報制御部

20 記憶装置

21 内線属性テーブル

22 RSA接続テーブル

23 パスワードコードテーブル

24 クラス定義テーブル

25 システムフラグテーブル

26 データテーブル

27 多機能電話ボタンテーブル

28 RSA接続先スクリーニングテーブル

30 28A 発信者スクリーニングテーブル

29 RSA録音メッセージテーブル

30 ネットワーク

31、32 トランク

T10 セキュリティ管理装置

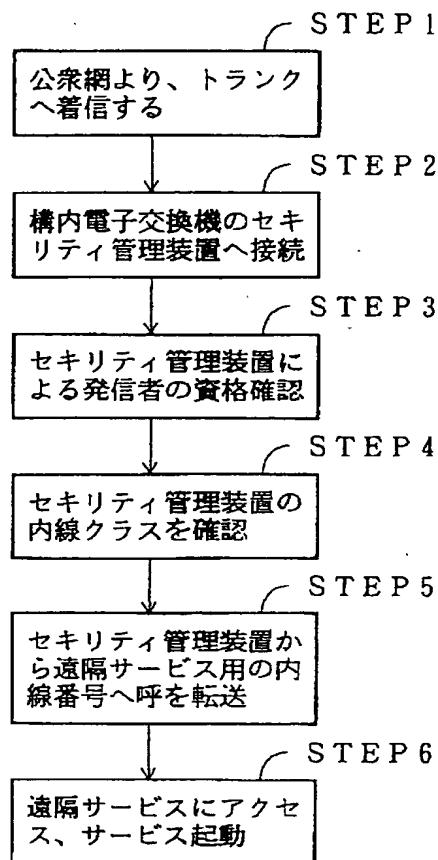
T20 録音装置

T30 多機能電話機

T1～Tn 端末

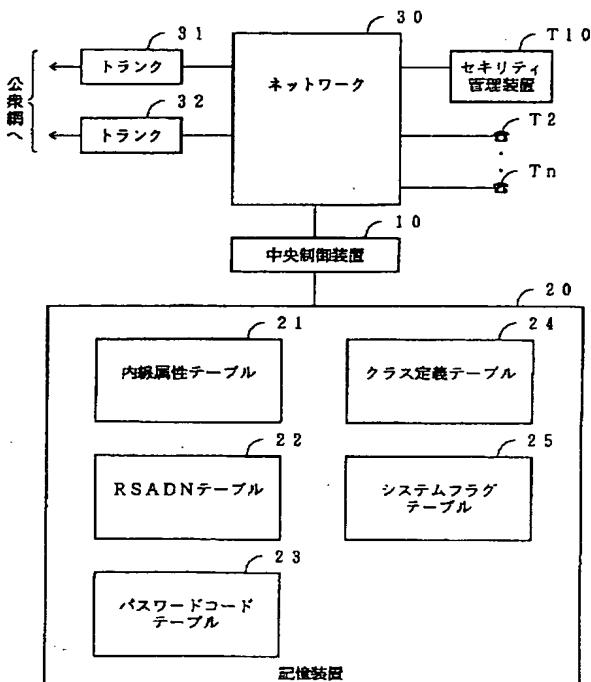
【図1】

本発明の原理を説明する図



【図2】

本発明の実施例の 内電子交換システム(1)を説明する図



【図3】

本発明の実施例のテーブル構成(1)を説明する図

(A)

	COS	RSM	FRL
内線A	0	1	6	.
内線B	1	5	0	.
.

(B)

RSADN	COS	RSM	FRL	SGRP
4000	2	3	3	1
.
.

(C)

PWC	COS	RSM	FRL
10BT	3	1	6
.	.	.	.
.	.	.	.

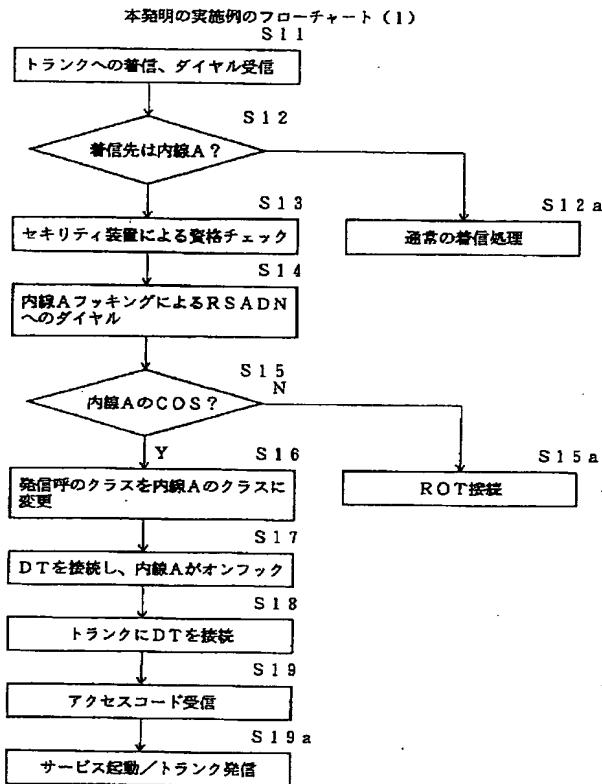
(D)

#-EXCOS	0	1	2
BSA転送	1	0	0
.	.	.	.

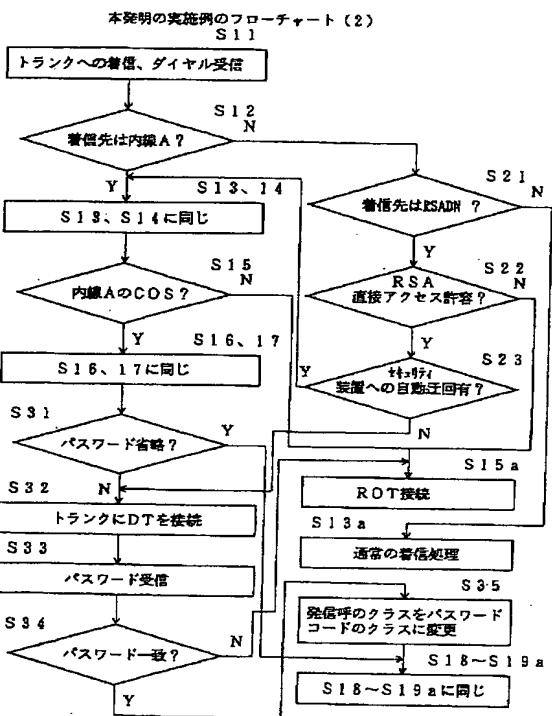
(E)

BSAへの直接アクセス許容タグ 251	0
セイテイ装置への自動巡回タグ 252	1
BSA-F-F省略タグ 253	1
.	.

[図4]

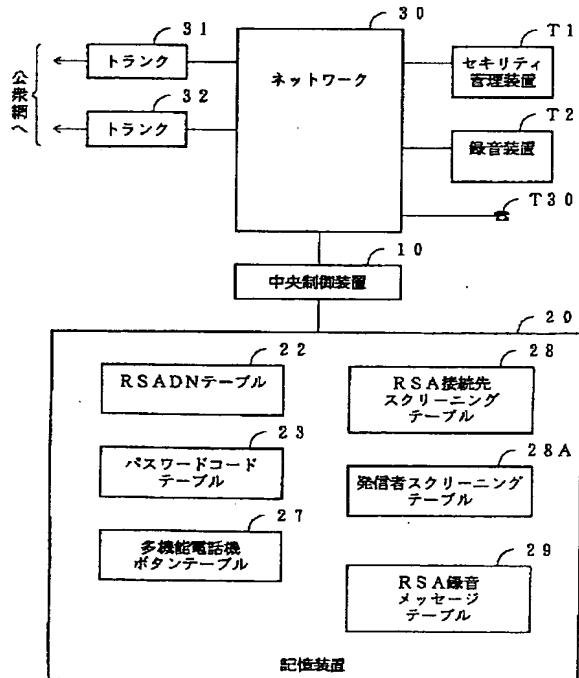


[四 5]

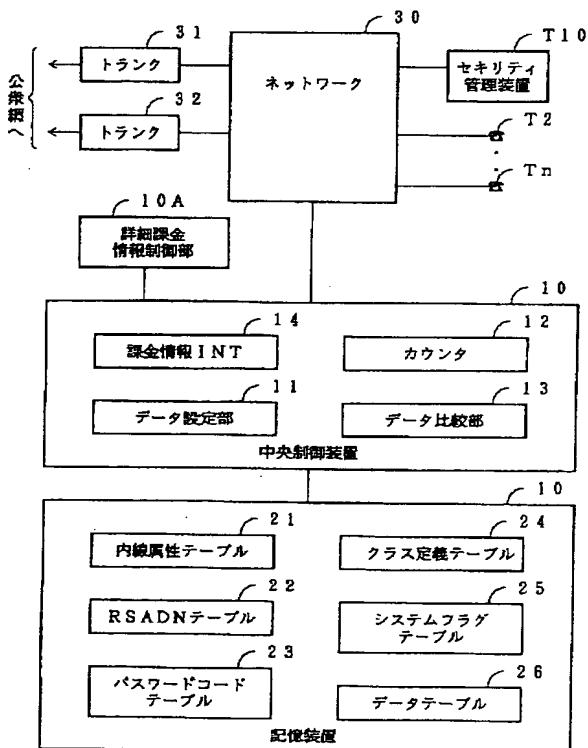


[9]

本発明の実施例の構内電子交換システム（3）を説明する図



本発明の実施例の構内電子交換システム(2)を説明する図



【図7】

本発明の実施例のデータテーブルを説明する図

パスワードコード	局線トランク発信回数		専用線トランク発信回数		RSAサービスへのトータルアクセス回数	RSAの使用累積料金	
	ルーティング先番号	回数	ルーティング先番号	回数			
12945	許容回数／料金	03 044 0457771111	5 5 8	4 3 74 70001234 79305678	20 10 10 5 5	150	30,000
	①			③	⑤	⑦	
	使用回数／料金	03 044 0457771111	3 2 2	4 3 74 70001234 79305678	11 6 3 1 2	61	6,420
	②			④	⑥	⑧	
98765	許容回数／料金	0 7	5 5	7 4 3 2	8 6 5 2	50	12,000
	①			③	⑤	⑦	
	使用回数／料金	0 ②	4 2	7 4 2	3 4 2	18	4,310
				④	⑥	⑧	
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

26

【図10】

本発明の実施例のテーブル構成(2)を説明する図

(A)

内線B	00 主回線
	01
	02 RSA管理
	⋮

27

(B)

宛先コード
01181
71
70
⋮

28

(C)

発番号
7149307660
3245567321
5642763715

28A

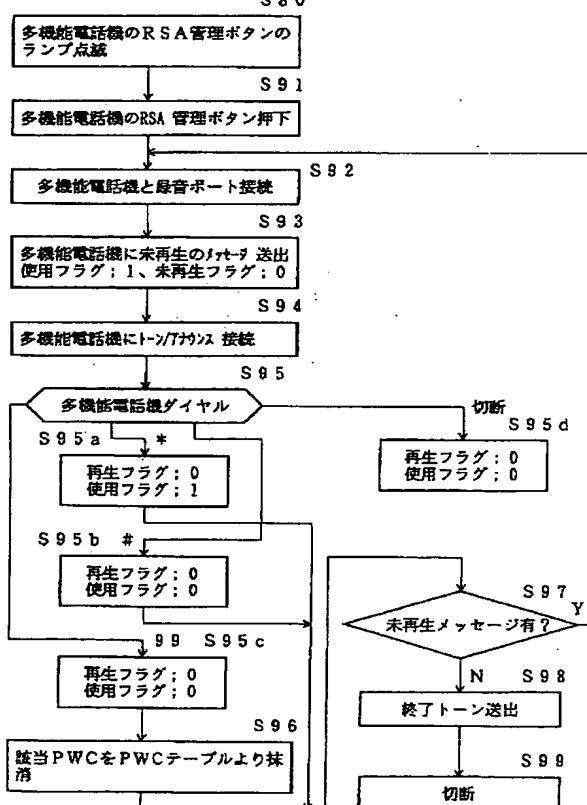
(D)

メッセージ番号	使用フラグ	PWC	ダイヤル番号	日時	再生フラグ
001	1	4589	01181		0
002	0	7932	711235		0

29

本発明の実施例のフローチャート(5)

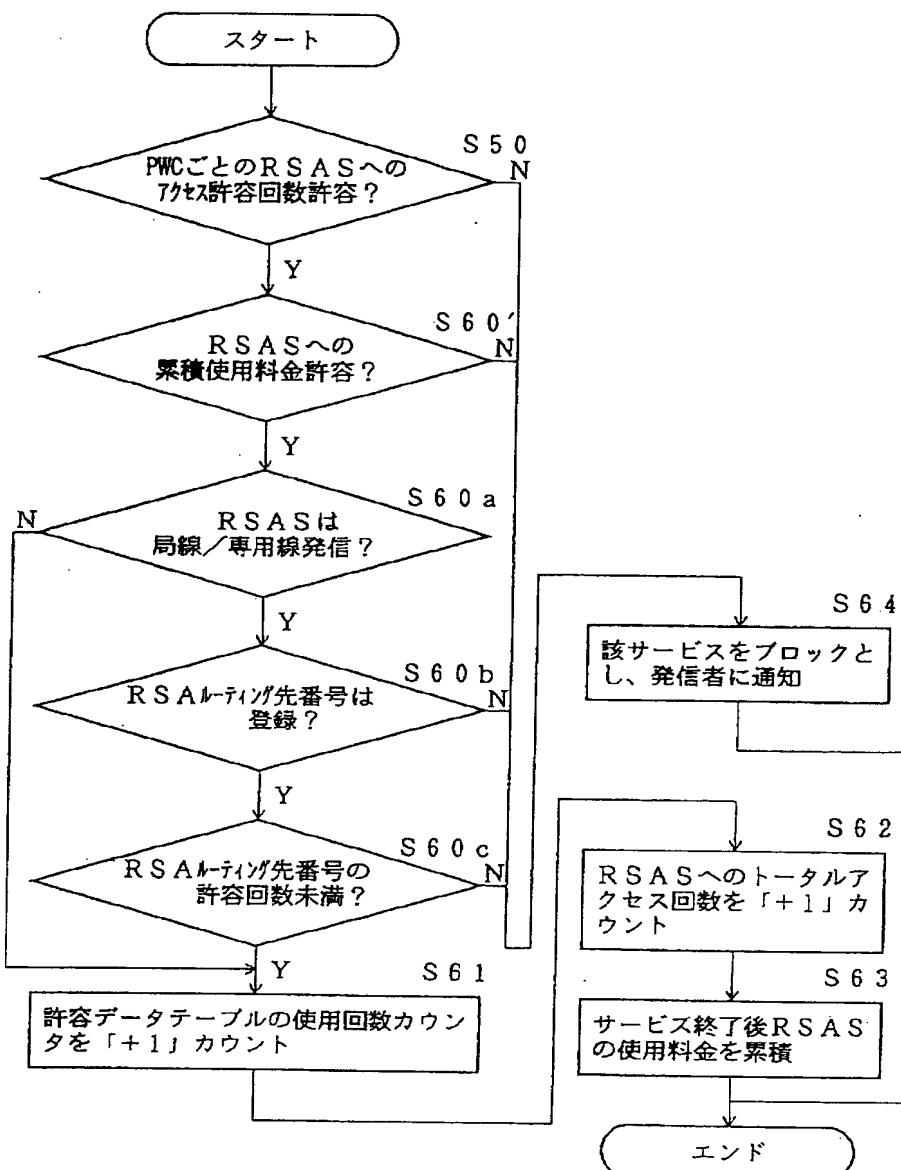
S80



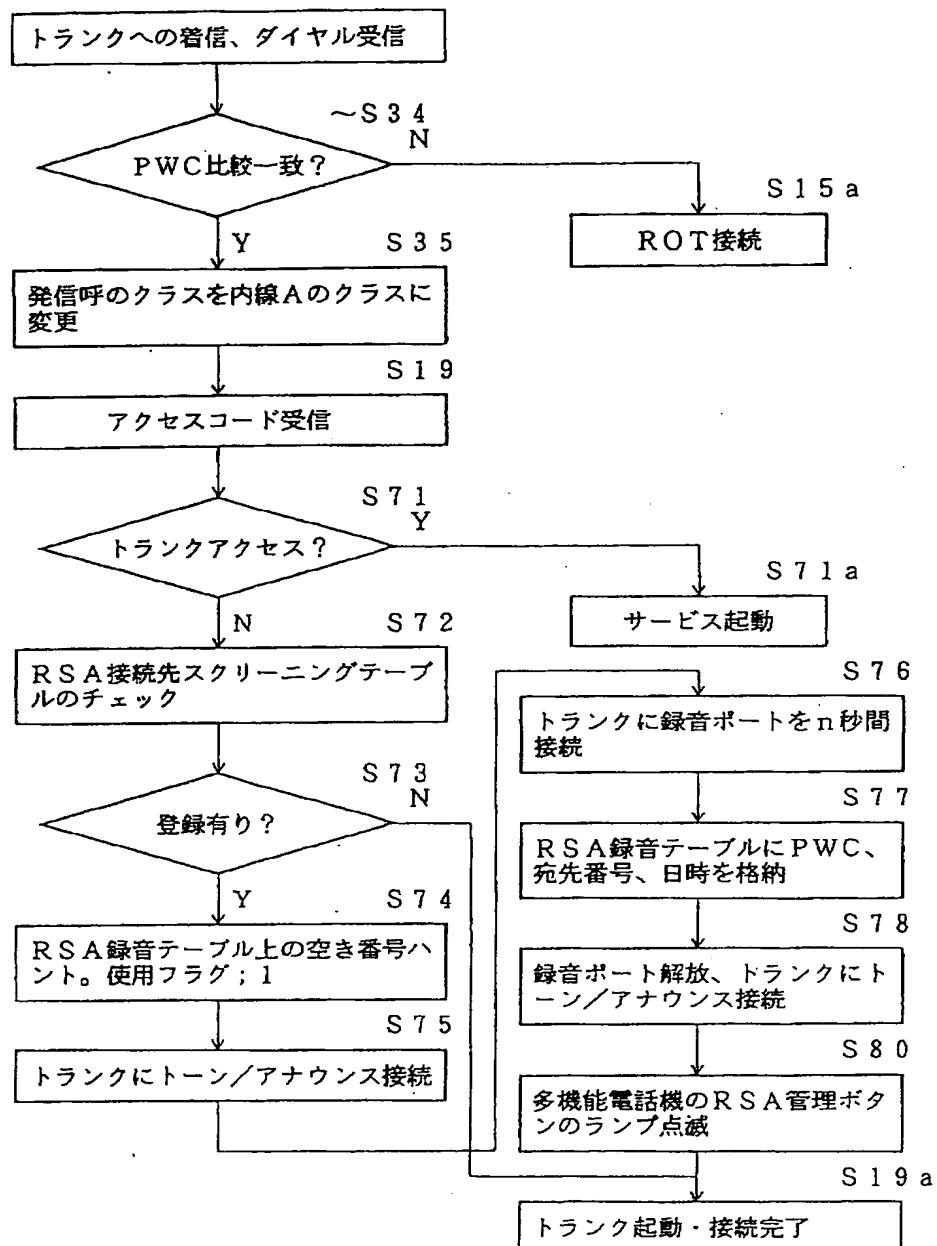
【図12】

【図8】

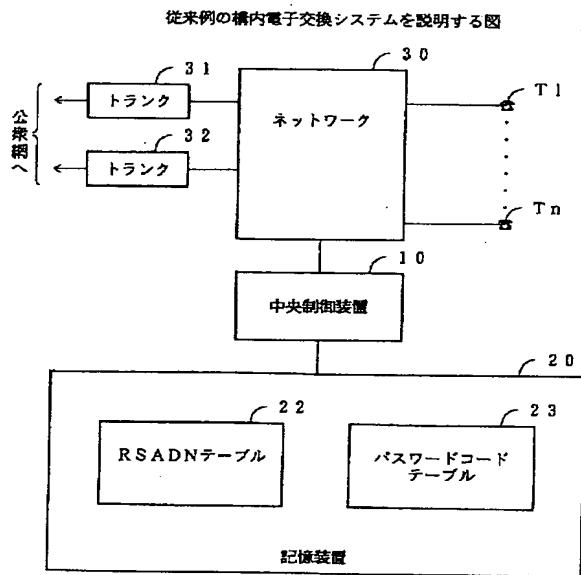
本発明の実施例のフローチャート(3)



【図11】

本発明の実施例のフローチャート(4)
S11~

【図13】



【図14】

